Department of Homeland Security Daily Open Source Infrastructure Report for 05 December 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports cyber criminals peddling illegal wares such as programs to hack into computers and stolen bank account numbers are moving to abandoned Websites where their activities are harder to track. (See item 3)
- The Transportation Security Administration has announced enhanced security screening procedures and changes to the prohibited items list that will allow additional explosive screening of shoes, hand−wanding of passengers, enhanced pat down searches, and inspections of carry−on bags. (See item 7)
- The Associated Press reports a bomb threat scrawled in the bathroom of an airplane at a gate at Newark Liberty International Airport on Friday, December 2, is believed to be an imitation of a similar threat that forced a jet to make an emergency landing in Kansas City a day earlier. (See item 9)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *December 03, Daily News (TX)* — **Refinery begins start−up process.** BP took its first steps toward restarting its Texas City, TX, oil refinery on Friday, December 2. The refinery, which

has been shut down since late September for a total overhaul, began producing steam overnight. Turbines from the massive electrical plant at the refinery were set to crank up Friday. The South Houston Green Power cogeneration plant, which is a joint venture of BP and Cinergy, will be in a warm−up mode for several days. That plant, in addition to generating electricity, produces the steam the refinery needs to operate. Steam is used to provide the heat for key process units. It also helps flare systems to burn cleaner. It will take several more days before the steam will make its way into the BP steam system at the Texas City refinery. Still, that process signifies an important marker for the refinery, which is on schedule to start a limited number of gasoline−producing units by year's end. Just before Hurricane Rita made landfall in late September, BP shut down the entire refinery. The company decided after the storm to take advantage of the shutdown to retool the entire facility.
Source: http://galvestondailynews.com/story.lasso?ewcd=60fd916d0cf5c 549

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

2. *December 02, Bureau of Engraving and Printing* — **New $10 bill to appear next year.** Redesigned Series 2004 $10 notes will be issued beginning on March 2, the Department of the Treasury and Federal Reserve Board announced on Friday, December 2. On this day of issue, Federal Reserve banks will begin distributing the new notes to the public through commercial banks. The announcement is a signal to businesses that handle cash and use machines that receive or dispense cash, to make final preparations for the new notes. For some businesses, getting ready for the new $10 note means training cash−handling employees on how to use the notes' updated security features; for others, the change involves making technical adjustments to machines that receive or dispense cash, such as vending and self−checkout machines. In order to stay ahead of counterfeiters, the U.S. government will redesign the currency every seven to ten years. Highlighted by images of the Statue of Liberty's torch and the words "We the People" from the U.S. Constitution, the new $10 note incorporates easy−to−use security features for people to check their money and subtle background colors in shades of orange, yellow and red.
Source: http://www.moneyfactory.gov/newmoney/main.cfm/media/releases 12022005

3. *December 02, Reuters* — **Cyber criminals gather on forgotten Websites.** Cyber criminals peddling illegal wares such as programs to hack into computers and stolen bank account numbers are moving to abandoned Websites where their activities are harder to track, security

experts say. Dormant Websites no longer monitored by administrators have in effect created hundreds of online bazaars for criminals, said Jim Melnick, director of threat intelligence for VeriSign Inc.'s security unit IDefense. Financial fraud cost consumers and businesses about nearly $15 billion in 2005 with some 10 million victims falling prey to identity theft, according to Avivah Litan of the market research firm Gartner. She said consumers recouped much of their losses, leaving businesses to pick up the tab. Security experts say they fear cyber criminals in the market for stolen financial and personal information will soon shift their sights to the hard−to−track locations. Making it more difficult for authorities, the advertisements for stolen software or personal information often appear on Websites that typically raise little suspicion. For example, an active link for a Christian Rock group contains postings encouraging users to download something called Paypal Database Hacker v1.5, and another reads: "USA Citibank, HSBC and Paypal account forsell!!!"
Source: http://www.msnbc.msn.com/id/10284366/from/RSS/

4. *December 01, Federal Trade Commission* — **Shoe company settles charges over security breach.** Shoe discounter DSW Inc. has agreed to settle Federal Trade Commission (FTC) charges that its failure to take reasonable security measures to protect sensitive customer data was an unfair practice that violated federal law. According to the FTC, DSW's data−security failure allowed hackers to gain access to the sensitive credit card, debit card, and checking account information of more than 1.4 million customers. The settlement will require DSW to implement a comprehensive information−security program and obtain audits by an independent third−party security professional every other year for 20 years.
Source: http://www.ftc.gov/opa/2005/12/dsw.htm

[Return to top]

Transportation and Border Security Sector

5. *December 02, Associated Press* — **Note in airplane bathroom forces emergency landing.** An America West Airbus jet made an emergency landing at Kansas City International Airport (KCI) after someone left a note in the plane's bathroom that said: "Taliban is Here." The plane was flying from Phoenix to Boston Thursday, December 1, when a passenger saw the note, KCI spokesperson Joe McBride said. The FBI, airport police and the Transportation Security Administration responded and police dogs searched the plane. No one was detained or arrested, McBride said.
Source: http://www.usatoday.com/news/nation/2005−12−02−emergency−lan ding_x.htm

6. *December 02, Associated Press* — **Officials investigating Continental bag screening at Newark.** Federal officials are investigating whether luggage for a Continental Airlines flight out of Newark Liberty International Airport was improperly screened, a spokesperson for the Transportation Security Administration (TSA) said Thursday, December 1. TSA spokesperson Ann Davis said agents observed nine bags that were not properly being screened. She said the officials fully scrutinized and screened them before they were loaded onto the plane bound for Houston on Sunday, November 27. TSA personnel discovered the nine bags without agency clearance stickers in a room beyond the bomb detection machines. An inexperienced Continental ticket agent had sent the checked luggage to the wrong place, said officials. Davis said Sunday's incident needs to be investigated before the TSA determines whether it will fine

Continental. The Houston−based airline already faces $50,000 in penalties for three violations of federal screening mandates since October, she said.
Source: http://www.usatoday.com/travel/news/2005−12−02−newark−luggag e_x.htm

7. *December 02, Transportation Security Administration* — **TSA unveils enhanced security screening procedures and changes to the prohibited items list.** Beginning December 22, airline travelers can expect to see more random screenings, fewer prohibited items, and a Transportation Security Administration (TSA) workforce more dedicated to detecting and defeating more serious threats, such as explosives. These changes are part of an update to security procedures announced on Friday, December 2, by Assistant Secretary Kip Hawley, to address the ever−evolving threat to commercial aviation. The specific changes include more additional screenings of passengers and their bags using a variety of methods selected at random. Passengers will also once again be able to carry small tools and scissors on−board aircraft. These changes will allow TSA to focus resources on more serious threats. “It is paramount to the security of our aviation system that terrorists not be able to know with certainty what screening procedures they will encounter at airports around the nation,” said Hawley. “By incorporating unpredictability into our procedures and eliminating low−threat items, we can better focus our efforts on stopping individuals that wish to do us harm.” Examples of this additional screening include explosive screening of shoes, hand−wanding of passengers, enhanced pat down searches and inspections of carry−on bags. These searches will be generated at random and will take only about a minute to complete.
Source: http://www.tsa.gov/public/display?theme=40&content=090005198 018c349

8. *December 02, Associated Press* — **Airline didn't screen workers, faces fines.** US Airways faces fines of nearly $180,000 for failing to put employees through background checks before letting them work in secure areas. The Transportation Security Administration is investigating the case, and the airline said it has received formal notification that it will face the penalties. The violations date from 2002 and 2003 at the former America West Airlines, now US Airways. The companies combined in September. Federal regulations enacted after the September 11, 2001 terrorist attacks require airlines to do criminal background checks on employees with access to secure areas.
Source: http://www.usatoday.com/travel/news/2005−12−02−usair−screeni ng_x.htm

9. *December 02, Associated Press* — **Threat forces evacuation of plane at Newark gate.** A bomb threat scrawled in the bathroom of an airplane at a gate at Newark Liberty International Airport on Friday, December 2, is believed to be an imitation of a similar threat that forced a jet to make an emergency landing in Kansas City a day earlier, authorities said. Continental Airlines flight 2499, which had been scheduled to depart for Pittsburgh at around 12:20 p.m., was towed to a remote section of the airport, where it was searched for explosives before being cleared at 1:50 p.m. EST, said Tony Ciavolella, a spokesperson for the Port Authority of New York and New Jersey, which operates the airport. Twenty passengers who were on the aircraft at Terminal C were removed and questioned by investigators while the search was being carried out. They were taken back to the terminal by bus, and were placed on a different plane, which took off at 3:15 p.m. to make the flight to Pittsburgh. The threat came a day after an America West Airbus jet made an emergency landing at Kansas City International Airport when someone left a note in the plane's bathroom that said: "Taliban is Here."
Source: http://www.usatoday.com/travel/news/2005−12−02−bomb−threats_x.htm

10. *December 02, Agence France−Presse* — **Distraught Canadian trucker drives off with missile launchers.** A truck driver suffering from marital problems drove off with a cargo of military personnel carriers armed with missile launchers before Canadian police stopped him near Toronto, officials told Agence France−Presse. The military vehicles were supposed to be transported from Canadian Forces Base Meaford, north of Toronto, to Montreal this week where they would be placed in storage, said Major Daryl Morrell. Instead, the driver, employed by a civilian trucking firm, was headed in the opposite direction on a busy highway when he was pulled over by a half dozen police cruisers and arrested. Police impounded the flatbed semi−trailer truck and its cargo, but did not charge the driver. The missile launchers can destroy ground targets over long distances, but there was no ammunition on the truck, Morrell said. As for the security breach, he said, "We see this as an isolated incident, but we will be discussing it with the contractor."
Source: http://news.yahoo.com/s/afp/20051202/wl_canada_afp/canadamilitaryarms_051202232653

11. *December 01, Register (UK)* — **EU ministers approve biometric ID, fingerprint data sharing.** The European biometric ID card took another step forward with the European Justice and Home Affairs Council set to approve "minimum security standards" for national ID cards. Alongside this, the Council will be road mapping the rollout of Europe's biometric visa system, which will contain the fingerprints of 70 million people within the next few years, and hearing European Commission proposals for greater sharing of fingerprint data. The latter proposals cover the existing Schengen Information System, its Visa Information System successor (VIS/Schengen II), and the EURODAC database of asylum seekers and illegal immigrants. The Commission will also be raising other initiatives including the consideration of a system for monitoring entry and exit movements, a frequent traveler system, and the creation of an European criminal Automated Fingerprints Identification System. So although some European states (not the UK) are strongly against the creation of a central biometric database of all their citizens, the construction of large−scale pan−European fingerprint systems proceeds apace.
Source: http://www.theregister.co.uk/2005/12/01/jahc_biometric_id_st andards/

[Return to top]

Postal and Shipping Sector

12. *December 02, Computerworld* — **FedEx expands global wireless strategy.** FedEx Express, a subsidiary of FedEx, has expanded its global wireless strategy with the planned rollout of the FedEx PowerPad across the international network. This expansion will build on the success of the pilot program in Hong Kong, which has already completed deploying the devices. FedEx PowerPad will replace the current hand−held courier device, the FedEx SuperTracker, and will act as a personal gateway to convey data directly to and from the FedEx internal network. Bluetooth wireless technology and a General Packet Radio Service (GPRS) connectivity network provide immediate information access, even when couriers are away from their delivery vans, revolutionizing the service level to customers by facilitating faster pick−ups. FedEx plans to globally deploy 50,000 devices to FedEx couriers by 2008 and over 2,500 FedEx PowerPads will be deployed in Asia Pacific, namely Hong Kong, Singapore, Taiwan, Japan, Australia, Malaysia, Korea, New Zealand, Guam, and Macau, to ensure every courier

will have his own device. The initial FedEx PowerPad deployment includes electronic signature capture, electronic pickup manifest, hands−free data transmission, and automatic scan transmission. The new device also enables dispatchers to schedule customer pickups faster and more efficiently.
Source: http://computerworld.com.sg/ShowPage.aspx?pagetype=2&articleid=3124&pubid=3&issueid=75

13. *December 02, Times−Standard (CA)* — **Detectives looking for post office bandit.** A postal worker was assaulted early Wednesday morning, November 30, when the employee tried to stop a man from breaking into parcel lockers at the West Clark (CA) Post Office. The Eureka, CA, police department said the employee saw a man walk into the lobby around 5 a.m. PST and forcibly open the parcel lockers. As the employee approached the man and tried to restrain him, a fight ensued. No weapons were used, but the man assaulted the postal employee. The employee received minor injuries that did not require medical attention. The man got away and the employee followed, but lost him after a short chase. Eureka police detective Dave Parris and U.S. postal inspectors are working on the case.
Source: http://www.times−standard.com/local/ci_3272144

14. *December 02, CBS2 (IL)* — **Suspicious post office package was medical sample.** A suspicious package at a downtown post office resulted in a Hazmat response in Chicago, IL, on Friday, December 2. No one was injured and officials who secured the scene later determined that the package contained a medical sample. Medical samples are commonly sent via mail.
Source: http://cbs2chicago.com/topstories/local_story_336105714.html

15. *December 01, Star Tribune (MN)* — **Minnesota soldier accused of shipping AK−47s home.** A Minnesota Army National Guard soldier illegally shipped two AK−47 assault rifles to the United States from Iraq, according to indictments returned by a federal grand jury in Wisconsin this week. The indictments charge that 21−year−old Victor Melnichuk, a combat engineer with A Company of the 682nd Engineering Battalion, based in Litchfield, packed the weapons with other gear last January as his 30−member unit prepared to return to the United States after a year in Iraq. The sealed shipping container arrived at Fort McCoy in western Wisconsin near Sparta in April. Melnichuk's unit was assigned various construction projects that included building and guarding prisons, giving him access to enemy weapons, according to the U.S. attorney's office in Madison, WI. Shipping the AK−47s would be a federal firearms violation. A federal grand jury in Madison indicted Melnichuk on two charges: illegally importing the assault rifles and illegally possessing them. If convicted, he faces up to five years on the importation charge and up to 10 years on the possession charge.
Source: http://www.startribune.com/stories/467/5758268.html

[Return to top]

Agriculture Sector

16. *December 03, Rockford Register Star (IL)* — **Six chronic wasting disease cases found in Illinois.** Illinois has had six new cases of chronic wasting disease (CWD) from samples taken during the hunting season, bringing the total to 102 since the fatal deer ailment was first

discovered near Roscoe in 2002. Four new cases were from the Winnebago−Boone county line and were deer taken during the first firearm season. They came from about 200 tests completed as of Tuesday, November 29. Hundreds of other samples still are being tested as the state hopes to examine about 2,000 deer killed in the firearm seasons. One other positive test was from a deer killed by a Boone County bow hunter, and the other one was a suspect deer killed by wildlife officials in Winnebago County. During last year's firearm season 31 deer tested positive, which was 20 fewer than in 2003. Paul Shelton of the state Department of Natural Resources said it was too early to say if this year's figures indicate a continued downward trend. However, he was encouraged because no new cases were found outside of previously infected areas.
CWD information: http://www.cwd−info.org/
Source: http://www.rrstar.com/apps/pbcs.dll/article?AID=/20051203/SPORTS19/112030032/1155/SPORTS

17. *December 01, Associated Press* — **Low−grade flu found in turkeys at North Carolina farm.** Turkeys at farm in eastern North Carolina have tested positive for antibodies for a low−grade strain of flu, but state health officials stressed there was no danger to people or other animals. "This isn't even a bird flu virus," state veterinarian David Marshall said Thursday, December 1. "It is one of many types or strains (of influenza) that can birds can be exposed to. ... It's something we typically find several times a year not only here, but in other states." Routine blood tests on birds from bound for slaughter in mid−November found antibodies for the H3N2 strain of flu. That strain is considered a low−enough risk that the U.S. Department of Agriculture requires no action, such as quarantine or destruction of livestock, Marshall said. The Sampson County farm where the turkeys were grown was quarantined for a couple of days while state officials confirmed the type of virus involved, Marshall said.
Low pathogenic avian influenza virus information:
http://www.aphis.usda.gov/lpa/pubs/fsheet_faq_notice/fs_ahlp ai.html
Source: http://www.myrtlebeachonline.com/mld/myrtlebeachonline/13304 469.htm

[Return to top]

Food Sector

18. *December 02, Los Angeles Times (CA)* — **Lettuce the likely culprit in new hepatitis A cases.** Health officials on Thursday, December 1, identified lettuce as the likely source for a hepatitis A outbreak in Los Angeles, CA, and urged residents to thoroughly wash the vegetable before eating it. At least 60 people have fallen ill from the virus in Los Angeles over the last three months. Officials are concerned because the outbreak comes after years of declining hepatitis A cases, but they have been unable to link the outbreak to a particular farm or type of lettuce. There were at least two outbreaks: one in a downtown Los Angeles restaurant in September that affected 13; the other at an event catered by a Hollywood company in October where 19 fell ill. The other cases were scattered. Outbreaks are hard to track, because the disease has a two− to eight−week incubation period. Infected people start showing symptoms after a month. Symptoms include fever, chills, aches, fatigue, nausea, vomiting, abdominal cramps, dark urine and jaundice.
Source: http://www.latimes.com/news/local/la−me−lettuce2dec02,0,6076437.story?coll=la−home−headlines

19. *December 01, Food Safety and Inspection Service* — **Lunchmeat products recalled.** ConAgra Foods, a Marshall, MO, firm, is voluntarily recalling approximately 9,550 pounds of various bologna, ham, and turkey lunch meal products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Thursday, December 1. The bologna, ham, and turkey products were produced on various dates between November 18 and 23 and were distributed to retail establishments nationwide. The problem was discovered through the establishment's microbiological testing. FSIS has received no reports of illnesses associated with consumption of the products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_052_2005_relea se/index.asp

[Return to top]

Water Sector

20. *December 05, CBS 11 News (TX)* — **Four hundred violations found in Texas water systems.** A media inquiry into water quality violations in Texas found that since the middle of 2004, 400 Texas water utility systems have been cited by the Commission on Environmental Quality for non−compliance. The citations were distributed to the Gulf Coast community of Surfside, areas within the Arkansas border region in far northeast Texas, and many sites in between. Violation notices indicated that two kinds of chemicals −− Trihalomethanes (TTHM) and Haloacetic Acids (HHA5) −− were higher than rules allowed, and announced for the first time ever that long−term exposure "may" cause liver, kidney and rectal cancer, birth defects, and nervous system problems. The non−compliance records showed that more than 100 of the systems had twice the allowed level of one or both carcinogens and that more than 30 others tested at three times the minimum level, despite ongoing efforts to clean up their water. As of this summer, Central Texas communities in Coke County, Runnels, Three Rivers, Robert Lee, and Paint Rock were registering TTHMs and HAA5 in the water at five, six, and seven times the allowable limit.
Source: http://cbs11tv.com/topstories/local_story_334222526.html

21. *December 02, Environmental Protection Agency* — **Environmental Protection Agency launches online water security database.** The Environmental Protection Agency has announced the launch of the new Water Contaminant Information Tool (WCIT) database. The secure, online database for contaminants of concern to drinking water and wastewater (water) security is designed to assist users in planning for, and responding to, drinking water contamination threats and incidents. It provides current, reliable, contaminant data from peer reviewed sources and research. The database currently contains data for 48 contaminants. It includes information on water contaminants data including contaminant names, contaminant availability, fate and transport, health effects and toxicity, medical information, potential water quality and environmental indicators, sampling and analysis, and helpful response advice for utilities. Information on wastewater treatment and infrastructure decontamination will be added to this tool in 2006. WCIT access will be granted to drinking water and wastewater utilities, state drinking water and wastewater programs, drinking water and wastewater associations, and federal officials (including government laboratory personnel). Given the sensitivity of the

WCIT data, access to the tool will be tightly controlled with a password−protected feature, yet it will be readily available to these groups.
Tool: http://www.epa.gov/wcit
Source: http://www.epa.gov/wcit

22. *November 29, The Examiner (CA)* — **Largest water project in the western United States approved for San Francisco.** The largest water project in the western United States −− a multibillion−dollar plan to upgrade San Francisco's (CA) water system that aims to ensure a reliable supply for 2.4 million Bay Area residents until 2030 −− took final shape Tuesday, November 29. The San Francisco Public Utilities Commission signed off on the project's first comprehensive blueprint, which lays out a $4.3 billion price tag, a 2015 completion date, and general plans for more than 75 separate dams, tunnels, pumping stations and other upgrades. The project will focus on hardening the aging Hetch Hetchy water system against a major earthquake, improving its capacity and reliability. Studies have shown a large temblor could knock out the system for as much as 60 days. It carries water 167 miles from the Hetch Hetchy Valley in the Sierra to four counties in the Bay Area, including San Francisco and San Mateo.
Source: http://www.sfexaminer.com/articles/2005/11/30/news/20051130_ne06_hetch.txt

[Return to top]

Public Health Sector

23. *December 04, MosNews (Russia)* — **Ukraine declares emergency state in Crimea after bird flu confirmation.** President Viktor Yushchenko declared a state of emergency in parts of the Ukrainian region of Crimea on Saturday, December 3, after outbreaks of bird flu were recorded in the regions. The state of emergency decree followed a conference that considered urgent measures to counter the disease. Bird flu cases of the H5 variety have been discovered in Ukraine's southern Crimea peninsula according to preliminary test results. The H5 virus strain was found among domestic chickens and geese in the regions of Sovetskyi and Nizhnegorsky in Crimea. The preliminary test results will be forwarded to laboratories in England and Italy for further testing to determine if the virus is of the H5N1 strain that has killed more than 60 people in Asia and spread to Europe. Agriculture Minister Olexander Baranovsky told Ukrainian television that scores of domestic poultry had died in three regions of the peninsula and tests were being performed to determine the cause of death.
Source: http://www.mosnews.com/news/2005/12/04/fluemergency.shtml

24. *December 03, Agence France−Presse* — **Indonesia confirms eighth bird flu death.** A 25−year−old Indonesian woman who died Wednesday, November 30, has been confirmed by World Health Organization (WHO) tests as being the country's eighth bird flu victim, the health ministry has announced. Five bird flu sufferers are still alive in Indonesia, while six people are suspected of having the virus. The latest victim, Sri Wahyuni, was admitted to Sulianti Saroso Hospital, Indonesia's main facility for treating bird flu patients, on November 24 after being treated at a hospital on the outskirts of the capital for three days. Indonesia has launched a national drive that it says will involve millions of people at village level monitoring and helping to stamp out the spread of bird flu.
Source: http://news.yahoo.com/s/afp/20051203/hl_afp/healthfluindonesia_051203135607;_ylt=Ap_Xd8S2b7psJ4g_QnjafJ2JOrgF;_ylu=X3oDM

TBiMW04NW9mBHNlYwMlJVRPUCUl

25. *December 02, Reuters* — **X−rays show shared symptoms among bird flu victims.** The lungs of avian flu victims are racked by infections, clogged with pus, and surrounded by fluid, and the severity of the symptoms can predict whether the patients will survive, researchers said on Friday, December 2. Based on chest X−rays performed on 14 Vietnamese bird flu patients admitted to Ho Chi Minh City Hospital −− nine of whom died −− researchers at the University of Oxford in England found shared abnormalities that were good predictors of whether the disease would be fatal. The infection from the H5N1 avian flu virus caused multiple lung infections, "which usually represents pus and infection in patients with fever and a cough," radiologist Nagmi Qureshi said. "We also discovered that the severity of these findings turned out to be a good predictor of patient mortality." Three of the five surviving patients in the study, which was presented at the annual meeting of the Radiological Society of North America, underwent more detailed computed tomography (CT) exams after they left the hospital. Those images showed that while their respiratory symptoms had subsided, scar tissue formed in their lungs similar to damage suffered by victims of Severe Acute Respiratory Syndrome (SARS).
Source: http://abcnews.go.com/US/wireStory?id=1366678

26. *December 01, Food and Drug Administration* — **Food and Drug Administration approves first test to screen for West Nile Virus.** The Food and Drug Administration (FDA) Thursday, December 1, announced the approval of the first West Nile Virus (WNV) blood test to screen donors of blood, organs, cells, and tissues. The Procleix WNV Assay detects viral genetic material (ribonucleic acid or RNA). This new test will help protect patients who receive blood and other such products against West Nile infection. To date, there have been 30 documented cases of people who most likely acquired WNV from a blood transfusion, including nine who died. WNV is typically transmitted to humans by mosquito bites. It was first detected in the U.S. in 1999, and has reoccurred each year for seven consecutive years, causing close to 20,000 human cases of disease and at least 762 deaths since 2002. It is estimated that between one and two million people have been infected with WNV. In 2002, it was discovered that WNV could be transmitted in blood and an urgent effort to develop a blood test began.
Source: http://www.fda.gov/bbs/topics/NEWS/2005/NEW01266.html

27. *December 01, Agence France−Presse* — **Worries for key anti−malaria drug as resistance signs emerge.** Misuse of the world's most important anti−malaria drug is helping the disease's mosquito−borne parasite become resistant to the treatment. Artemisinin, derived from a Chinese herb, has become the drug of choice for treating malaria after chloroquine, introduced in the 1950s, was rendered useless by resistance. Researchers from the French−led Pasteur Institute Network took blood samples in 2001 from 530 malaria patients in Cambodia, French Guiana, and Senegal, where there are different patterns of artemisinin use. They then tested the samples in lab dishes, exposing the parasite, Plasmodium falciparum, to a range of malaria drugs. Some samples from French Guiana and Senegal, where use of artemisinin is uncontrolled, showed signs of being insensitive to that drug. But samples from Cambodia, where the drug is controlled, showed no sign of resistance. The new research pinpoints the problem to mutations in a gene in the parasite called SERCA−type Prtpase6 that is targeted by artemisinin. Resistance by a bacteria, virus, or parasite is encouraged when a patient fails to take a full course of drugs or uses drugs that are counterfeit or diluted.
Research report: http://www.thelancet.com/journals/lancet/article/PIIS0140673

605677872/fulltext
Source: http://news.yahoo.com/s/afp/20051201/hl_afp/healthmalariadrugs_051201230729;_ylt=AoJBiomJh7CfbwGEtE1XvYSJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

28. *December 01, Mid Hudson News (NY)* — **Search and rescue building collapses as part of drill at Yonkers Raceway in New York.** New York's Southern Westchester County Special Operations Task Force and the state's Capital District Urban/Technical Search and Rescue Team (CD U/TSAR) held search and rescue exercises Thursday, December 1, at a collapsed building at Yonkers Raceway. More than 100 area firefighters, four K−9 Unit search and rescue dogs and experts from the New York State Department of State's Office of Fire Control and Prevention participated in the drills. Yonkers, New Rochelle, Mount Vernon, White Plains, Eastchester/Scarsdale and Greenville/Fairview/Hartsdale Fire Departments make up the six squads of the Southern Westchester County Special Operations Task Force that have received special training and equipment to support a regional response to technical rescue incidents. The exercise scenario involved an actual collapse of a portion of a structure and was intended to better prepare responders. The drill was also conducted to evaluate the capabilities and capacities of the local responders, as well as the ability of the CD U/TSAR Team to interact with and augment local resources.
Source: http://www.midhudsonnews.com/News/Search_rescue−01Dec05.htm

29. *December 01, Journal News (NY)* — **Indian Point drill shows few problems.** New York emergency officials simulated a release of radioactive cooling water at the Indian Point nuclear plants Wednesday, November 30, to test the response capabilities of the plants' operator and the four counties surrounding the site. Though an official assessment won't be made until the state reviews all reports from its nearly 50 observers, officials from the New York State Emergency Management Office said the nine−hour drill turned up "no major flaws." Emergency officials from Westchester, Putnam, Rockland and Orange Counties participated in the exercise. "We always view these as good opportunities to sharpen our skills," Entergy spokesperson Jim Steets said. "It allows us to train new people and work with the counties. You always learn something from these things. The whole idea is to improve." One area that needed improvement was a telephone link between the plants and the counties, said Anthony Sutton, Westchester's top emergency official. Drill participants had to go to a backup line because the volume on the primary line wasn't loud enough for everyone to hear.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20051201/NEWS09/512010341/1025

[Return to top]

Information Technology and Telecommunications Sector

30. *December 02, Security Focus* — **Cisco IOS HTTP service HTML injection vulnerability.** Cisco IOS HTTP service is reportedly prone to an HTML injection vulnerability. An attacker can submit malicious HTML and script code through the '/level/15/exec/−/buffers/assigned' and /level/15/exec/−/buffers/all' scripts. This code may be executed in the browser of an administrator when they attempt to view the contents of memory buffers through the vulnerable scripts of the HTTP service. This vulnerable has been reported to affect versions of IOS from 11.0 through 12.4. Cisco IOS XR is not vulnerable. As this is a HTML injection vulnerability that targets users of the IOS Web interface, devices with the HTTP service disabled are not affected.
Source: http://www.securityfocus.com/bid/15602/references

31. *December 02, eWEEK* — **IE design flaw lets hacker crack Google.** An unpatched design flaw in Microsoft Corp.'s Internet Explorer browser could give malicious hackers an easy way to use the Google Desktop application to covertly hijack user information. The vulnerability was discovered in the cross−domain protections in Internet Explorer and a proof−of−concept exploit has been published. A spokesperson for Microsoft acknowledged the flaw in a statement and said the company was unaware of active attacks against IE users. The hacker who discovered the vulnerability used the Google Desktop utility to prove his findings, but in theory, any domain or application that depends on the IE cross−domain security model is vulnerable. Google spokesperson Sonya Boralv said initial investigations show that the problem resides in IE and not as a result of any vulnerabilities in Google Desktop, the downloadable utility that lets PC users merge desktop and search results on the well−known browser interface.
Source: http://www.eweek.com/article2/0,1759,1895579,00.asp?kc=EWRSS03129TX1K0000614

32. *December 01, Tech Web* — **Sober attack biggest virus outbreak ever.** Apparently, messages from the Federal Bureau of Investigation and Central Intelligence Agency are the way to spread worms, a security firm said Thursday, December 1, as it tallied up Sober's wildfire spread during November and concluded that the outbreak was the biggest ever. E−mail security provider Postini said that it had quarantined more than 218 million Sober−infected messages last week, more than four times the 50 million−message average that it blocks in a run−of−the−mill month. "This Sober generated close to a 1,500 percent increase in virus infected e−mail traffic in the past week," said Scott Petry, vice president of products and engineering at Postini, in a statement. Petry also said that Sober's attack was twice as large as the largest previous on Postini's records. Other security vendors took note of the recent Sober −− the variant is dubbed Sober.x, Sober.y, or Sober.z by most anti−virus firms −− and its impact during November. Both Sophos and Fortinet, for instance, had the new Sober at the top of their November charts as well.
Source: http://www.techweb.com/wire/security/174403317;jsessionid=0EZ1TE0ZK20WWQSNDBGCKHSCJUMEKJVN

33. *December 01, InfoWorld* — **Telecom experts call for reduced regulation.** Current U.S. government communications regulations that create a dividing line between

telecommunications and Internet services make no sense and may be inhibiting the U.S. economy, a group of telecom experts said Thursday, December 1. The U.S. Congress needs to pass a comprehensive overhaul of telecommunications law, focused on removing regulations on carriers trying to provide enhanced broadband services such as video over IP, said panelists at a Forum on Technology and Innovation event in Washington, DC. Laws that impose regulations on telecommunication carriers need to be repealed when companies that provide so−called information services over Internet don't face the same rules, said Randolph May, senior fellow at the Progress and Freedom Foundation, a conservative think tank based in Washington, DC. For example, VOIP providers face little regulation, while traditional telephone service providers face significant regulation, May said. "The distinction between information services and telecommunication services is really quite metaphysical and has nothing to do, at all really, with how consumers in the marketplace look at these services," May said. The panel, made of up free market advocates, all suggested less regulation was better, with May saying competition among telecom and Internet carriers was growing almost daily.
Source: http://www.infoworld.com/article/05/12/01/HNtelecomregs_1.ht ml

34. *November 30, Security Focus* — **Perl Perl_sv_vcatpvfn format string vulnerability.** Perl is susceptible to a format string vulnerability. This issue is due to a failure of the programming language to properly handle format specifiers in formatted printing functions. An attacker may leverage this issue to write to arbitrary process memory, facilitating code execution in the context of the Perl interpreter process. This can result in unauthorized remote access. Developers should treat the formatted printing functions in Perl as equivalently vulnerable to exploitation as the C library versions, and properly sanitize all data passed in the format specifier argument.
Solution: http://www.securityfocus.com/bid/15629/solution
Source: http://www.securityfocus.com/bid/15629/references

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received reports of a phishing email scam that attempts to convince the user that it is from the Internal Revenue Service (IRS) by using a spoofed "From" address of "tax−refunds@irs.gov".

Upon clicking on the link provided in the email, the user is taken to a fraudulent site that looks like a legitimate U.S. government site. The user is then asked to provide personal information, such as their social security, credit card and bank pin numbers.

Users are encouraged to take the following measures to protect themselves from this type of phishing attack:

Do not follow unsolicited Web links received in email messages.

Contact your financial institution immediately if you believe your account/and or financial information has been compromised.

For additional information on ways to avoid phishing email attacks, US−CERT recommends that all users review the following:

Avoiding Social Engineering and Phishing Attacks at URL: http://www.us−cert.gov/cas/tips/ST04−014.html

Spoofed/Forged Email at URL: http://www.cert.org/tech_tips/email_spoofing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 6346 (gnutella−svc), 445 (microsoft−ds), 80 (www), 27015 (halflife), 139 (netbios−ssn), 135 (epmap), 25 (smtp), 65535 (Adoreworm) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer